EUROPEAN PATENT OFFICE
EUROPEAN PATENT APPLICATION NO. 0 999 528 A2

Int. Cl.[7]:	G 07 F 7/10 G 06 K 19/07
Filing No.:	99122157.3
Filing Date:	November 5, 1999
Publication Date:	May 10, 2000 Patent Journal 2000/19
Priority	
Date:	November 5, 1998
Country:	DE
No.:	19851074
Designated Contracting States:	AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LI, LU, MC, NL, PT, SE
Designated Extension States:	AL, LT, LV, MK, RO, SI

SYSTEM AND METHOD FOR SECURE IDENTIFICATION AND REGISTRATION OF PERSONS, ESPECIALLY FOR ISSUING PERSONALIZED AUTHORIZATION MEANS, SUCH AS A DIGITAL SIGNATURE CARD, AND ALSO A REGISTRATION DEVICE SUITABLE FOR SUCH A SYSTEM

Inventor:	Ingvar Wagner 63128 Dietzenbach, DE
Applicant:	Elsdale Limited St. Heller, Jersey, GB
Agent:	Winter, Brandl & Partner Patent Attorney and Attorney at Law Chambers Alois-Steinecker-Strasse 22 85354 Freising, DE

[Abstract]

Disclosed is a system in a method for secure identification and registration of persons, especially for issuing personalized authorization means, such as a digital signature card. The secure registration is performed in a system comprising an authorization issuer, for example, a trust center, and at least one registration office, wherein the authorization issuer and registration office are linked in an authentication system, which guarantees that the registration can be performed only from registration offices authorized by the authorization issuer. This is achieved in that personalized data are read from a document identifying the registrant, wherein the document for identification contains at least one biometric feature of the person. The biometric feature detected from the identifying document is also detected or made on site from the person present. A verification unit compares the data detected directly on site with the data detected from the identifying document and determines with a certain likelihood whether the person applying for registration is actually the person present.

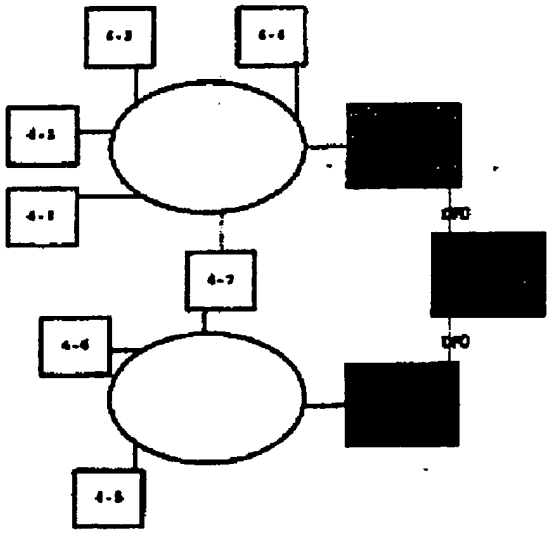


Figure 1

[0001]

The invention relates to a system and to a method for secure identification and the registration of persons, especially for issuing personalized authorization means, such as a digital signature card, as well as a registration device suitable for such a system.

[0002]

The law for digital signatures (signature law) regulates the initial conditions, according to which digital signatures, certificates, and time stamps are issued. Therefore, there is a need for legally conforming devices, systems, and methods for secure identification and registration of persons, so that it is guaranteed that authorizations, such as digital signatures, are issued only to positively identified persons. Because questions of liability arise for registration offices and trust centers (authorization issuers) when a signature card is issued to an unauthorized person, there is a need for a secure issuing method and system. The legal stipulations alone do not yet provide this security.

[0003]

From WO-A 98/28721, a device is known that detects personal data with, among other things, identification card readers, and processes these data for issuing additional personalized documents. However, in this way, it is not guaranteed that the detected personal data are actually the personal data of the person present. For example, an official identification card could have been read that does not belong to the person present.

[0004]

Therefore, the problem of the present invention is to disclose a system and a method for secure identification and registration of persons, especially for issuing personalized authorization means, such as a digital signature card, in which it is guaranteed that the authorization means or the release for issuing these authorization means is granted only to a positively identified person. Furthermore, the problem of the present invention is to disclose a registration device suitable for the system.

[0005]

The solution for this problem is realized by the features of Claims 1, 16, and 21, respectively.

[0006]

The secure registration is performed in a system comprising an authorization issuer for the issuing of digital signature cards, a so-called trust center, and at least one registration office, wherein the authorization issuer and registration office(s) are linked in an authentication system, which guarantees that the registration can be performed only by the registration offices authorized by the authorization issuer. Thus, "false" authorization means are prevented from reaching circulation. The registration offices here include registration devices according to the

invention, with which it can be positively determined whether a person applying for registration is actually the person that he claims to be. This is achieved in that personalized data are read from a document identifying the registrant, wherein the document for identification includes at least one biometric feature of the person, such as, e.g., a passport photo, a signature, a fingerprint, or the like. The biometric feature detected from the identifying document is detected on site from the person present, in that, e.g., a photo is taken of the person present or the person present gives a sample signature. According to an advantageous configuration of the invention, a verification unit compares the data obtained directly on site with the data obtained from the identifying document and determines with a certain likelihood whether the person applying for registration is also actually the person that he professes to be. The identity of the person applying for registration is determined with a certain likelihood, wherein it can be set with which likelihood the identity must be determined in order to grant the issuing of authorization means.

[0007]

According to an advantageous configuration of the invention, a higher-order authorization issuer (root), which is also linked into the authentication system, is allocated to the authorization issuers.

[0008]

According to another advantageous configuration of the invention, the programs and data for the application according to the invention are separated physically or virtually from other applications on the EDV [electronic data processing] systems of the authorization issuer and the registration offices. Alternatively, the EDV systems can also be used with their components exclusively for the secure identification and registration of persons for issuing authorization means. In this way, the possibility of manipulation is decreased.

[0009]

According to another advantageous configuration of the invention, the document reader in the identification unit tests the authenticity of the document read. This verifying can include both the physical authenticity by detecting watermarks, security threads, paper type, etc., and also the authenticity of the contents through comparison with external databases, etc.

[0010]

According to another advantageous configuration of the invention, the authentication system is realized in that both the authorization issuer and also the registration offices can be identified uniquely by means of a secure ID, e.g., in the form of an electronic key. That is, the

individual components of the system are identified uniquely with a secure ID in the form of an electronic certificate, in the form of a digital signature card, etc., whereby manipulation is made more difficult. According to another advantageous configuration of the invention, the individual components of the authorization issuer and the registration offices are also provided with individual secure IDs. In this way, switching of external components into this system with secure IDs can be securely prevented, so that manipulation is nearly completely impossible.

[0011]

According to another advantageous configuration of the invention, the secure ID of the authorization issuer is granted by the higher-order authorization issuer and the secure ID of the registration offices is realized by the higher-order authorization issuer. In this way, security against manipulation is also increased.

[0012]

According to another advantageous configuration of the invention, the secure IDs, the authorization issuer, the registration offices, and also the individual components are verified periodically or at certain events, so that it is always guaranteed that only "authorized" components and offices are linked into the system according to the invention.

[0013]

According to another advantageous configuration of the invention, the registration device is functional, i.e., registrations can be performed, only when both the secure ID of the relevant registration office and also the secure ID of the associated authorization issuer are present and have been identified as correct. In this way, security against manipulation is also increased.

[0014]

According to another advantageous configuration of the invention, the individual components of the EDV system or the registration devices can be activated only by "authorized" persons with a secure ID. That is, each operator must insert, for example, his personal digital signature card into the device and only if the corresponding hardware component recognizes the person identified by the digital signature card as an "authorized" person can the appropriate hardware component be activated or can the application program for registering and identifying the persons be initiated. Instead of a digital signature card, a special electronic key, password, biometric feature, etc., can also be used. In this way, security against manipulation is further increased.

[0015]

According to another advantageous configuration, electronic interfaces to the registration offices spare the "customer"—the registrant—from making his way to the local authorities; confirmations can be received online from home. The electronic interfaces to external and internal registration offices and databases can be used, in general, for comparing data, creating necessary data, and for feasibility tests. Through the ability for cashless payment by means of EFTPOS, the workload at the payment window and in the accounting department is lessened.

[0016]

According to another advantageous configuration of the invention, the registration device includes a chip-card processing device, by means of which the necessary data and information are inserted or loaded into the authorization means in the form of chip cards. This applies especially for the issuing of digital signature cards. Thus, authorization means in the form of cards can be provided with features on the surface or in the card. For example, the name of the authorized person can be printed, features can be printed in invisible text, or the photo of the authorized person is printed on the authorization means.

[0017]

According to another advantageous configuration of the invention, the identification units of the registration devices also include a device for capturing the dynamic response of a biometric feature. Thus, for example, the writing speed and the pressure distribution while the signature is being signed can be detected and verified. In this way, the likelihood with which the identity of a person is determined is further increased.

[0018]

With the method from Claim 21 according to the invention, the identity of a person applying for registration can be determined securely.

[0019]

According to another configuration of the invention, at the beginning of registration, the desired authorization means, e.g., digital signature card, can be selected. In this way, various authorization means can be issued or the release for the issuing can be granted with a single registration device.

[0020]

According to another advantageous configuration of the invention, the security of the identification is increased such that in addition to personalized data from an identifying document, personalized data from internal and external databases, such as, e.g., a register of residents, driver's license lists, a central register, CD-ROM, etc., are also included and verified for agreement. In addition, a dialog-controlled query for the registrant is also possible. Furthermore, necessary information, features, and attributes of the registrant can be read and processed from additional documents describing the registrant.

[0021]

According to another advantageous configuration of the invention, the obtained data can be displayed and/or printed. This can be performed merely for information or in the form of a request, which can then also be signed.

[0022]

The system according to the invention is suitable especially for issuing a digital signature card according to Claim 32. Here, the person who is applying for a digital signature card, is first positively identified by the method according to the invention. In addition, PSE data are read from a pre-initialized chip card and are transmitted to a software program. Through the software, the personalized data of the positively identified requester are combined with the PSE data, and the data necessary for issuing the digital signature card are displayed on a legally conforming display. Then the relevant data are signed, encrypted, and transmitted to the authorization issuer. After verifying by the authorization issuer, the associated certificate is signed digitally and transmitted encrypted to the registration office. In the registration office, the transmitted data are decrypted and verified again and, in the case of a positive test result or in the case of release by the authorization issuer, the necessary data are transmitted with the certificate to the pre-initialized chip card and this card is personalized. Then the instructions prescribed by law are given and a confirmation that the instructions were given and a receipt for the digital signature card are printed.

[0023]

According to an advantageous configuration of the invention, the uniqueness of the key contained in the PSE data of the pre-initialized chip card is checked by the authorization issuer either upon the transfer of the certificate or before.

[0024]

According to another advantageous configuration of the invention, the information provided with the issuing of the digital signature card is delivered via programmed, dialog-guided instruction with subsequent verifying. Only when the test has been completed successfully is the signature card activated. In this way, the legal requirements in terms of information are taken into account, and, at the same time, the expense for personnel for this legally required instruction is minimized.

[0025]

According to another advantageous configuration of the method according to the invention, a report to a third party is generated upon the issuing of an authorization means or upon a release for issuing an authorization means, e.g., in the form of a digital signature card. This is useful if this third person has hired or authorized the registrant, in order to allow additional authorizations, such as powers of attorney, to be registered in the corresponding authorization means. In this way, e.g., representatives of a company can be authorized electronically and the institution or person authorizing the representatives can be informed about this action.

[0026]

According to another advantageous configuration of the invention, the registration is ended automatically after successful completion of a registration, i.e., the device or the registration device deactivates itself or the registration is automatically stopped after a certain time period, because when a maximum time period for a registration is exceeded, a manipulation attempt is assumed.

[0027]

According to another advantageous configuration, each registration process and also the communications between the individual components of the system according to the invention are logged, so that manipulations or irregularities can be detected securely and certain persons can be associated with the actions. In addition, the logs and data are transmitted according to a certain scheme to the associated authorization issuer, which checks them for completeness and correctness or in order to determine possible manipulation and then transfers them to an electronic storage device. Thus, the entire archive of paper documents can be eliminated. A significant advantage, both for the registration offices and also for the authorization issuer. Electronic archiving and error-checking go hand-in-hand.

[0028]

According to another advantageous configuration of the invention, the obtained data and logs at the registration office are deleted according to a certain scheme, wherein the release for deletion is realized preferably by the associated authorization issuer. In this way, data protection is guaranteed and manipulation of the obtained data is excluded.

[0029]

The remaining subordinate claims relate to additional advantageous configurations of the invention.

[0030]

By allocating secure IDs and their exchange and verifying, manipulation and irregularities are nearly completely excluded, but at the least these can be associated with a responsible party by using evidence. In addition, the use of secure IDs renders the associated devices useless without these secure IDs. In the extreme case, such a hardware component is functional only when the secure ID of the authorization issuer, the secure ID of the associated registration office, the secure ID of the associated component, and the secure ID of an authorized user are present. Thus, there is no security risk even by theft or by resale of such a component to unauthorized third parties.

[0031]

The issuing of signature cards is a new process and it will be a long time before it is a routine process performed perfectly and with corresponding high quality. At the beginning, there will be "growing pains." The lack of experience by the masses and the necessary learning processes can cause high error rates, uncertainty by the "sellers," and misunderstandings by the new "customers." That is poison for market introduction. The system according to the invention simplifies the quality assurance in the registration and issuing of the card according to signature law and eases typical start-up difficulties. Through the extensive automation, but with the ability for operators to intervene, consistently high quality is guaranteed, which, for processes that are performed by aides only occasionally (e.g., 1 to 2 times a day), can be achieved only with much difficulty.

[0032]

The system and method according to the invention is more economical than the purely manual method. The predominantly manual and paper-supported methods are intensive in terms of persons and are therefore expensive. Included here are media disruptions, which represent, to

some extent, double work, and also always sources for errors. The costs for quality assurance are therefore high. According to requirements, the system according to the present invention is more economical than manual methods, starting at around 35 registrations/requests/cards per month. The superiority is based on the shortened processing times in the registration offices and at the authorization issuers (trust centers).

[0033]

The registration and card issuing according to the invention therefore has the following advantages relative to conventional methods:

the economy relative to other methods, especially manual;

the convenience of registration in comparison with other methods;

fulfillment of future legal regulations for authorization issuers and their aides;

[0034]

For the "seller," high process security is guaranteed, convenience is given to the "customer," and simplification of work, reduction of legal risks, and decreased costs for registration make a significant difference for the authorization issuers.

[0035]

Additional details, features, and advantages of the invention follow from the description below of an example embodiment of the invention with reference to the drawings.

[0036]

Shown are

Figure 1, a schematic representation of the entire system;

Figure 2, a schematic representation of a registration device in a registration office; and

Figure 3, a schematic representation for explaining the authentication system with secure IDs.

[0037]

Figure 1 shows a schematic representation of the system according to the invention with a higher-order authorization issuer 1, which can be connected by means of a data transmitting device (DFÜ) to two lower-order authorization issuers—also called trust centers—2-1 and 2-2 (drawn with dashes). The first authorization issuer 2-1 is connected by means of DFÜ to a plurality of registration offices 4-1 to 4-4. The second authorization issuer or the second trust center 2-2 is also connected by means of DFÜ to two registration offices 4-5 to 4-7. The

individual registration offices can also be connected to several authorization issuers 2i. This is shown for the registration office 4-7 as an example by the dashed connection.

[0038]

Each of the registration offices 4 comprises in turn at least one registration device 6, the structure of which is shown schematically in Figure 2. The registration device 6 comprises a control unit 8, e.g., in the form of a PC, a monitor 9, an input means 10 in the form of a keyboard or the like, an output means in the form of a printer 12, a first document reader 14, a second document reader 15, and a device 16 for on-site detection of a biometric feature of the registrant. The registration device 6 further comprises a verification unit 18, a card payment unit 20 with modem, a PIN input device 22, a device 23 for digitizing a signature, a chip-card processing device 24, a PIN output printer 26, a card personalizing unit 27, a DFÜ interface 28, an authentication unit 30, and an uninterruptable power supply 32.

[0039]

The first document reader 14 is used for reading personalized data from official identification cards and also comprises a unit for verifying the authenticity of the documents read. In addition, the document reader also captures photos, signatures, fingerprints, photos of the iris, etc., from identifying documents, which are then processed in the verification unit 18. The second document reader 15 is provided for other and non-official documents. The device 16 can be an electronic camera, a device for recording fingerprints, a device for photographing the iris or the like. The device 23 for digitizing a signature can be used for active detection of the biometric feature "signature" and also for signing a request for issuing a digital signature card. In this way, the signature is simultaneously recorded electronically and added to the electronic documents as an image and digitized. By means of the PIN input unit 22, an authorized operator Bi and the registrant can be identified by means of a PIN already assigned to him. The PIN input unit represents a component of a knowledge-based and learning identification system.

[0040]

By means of the authentication unit 30 and the DFÜ interface 28, the registration device 6 can be connected to the associated authorization issuer 2. By means of the DFÜ interface 28, the registration device 6 can also be connected to external databases 36, which can be, for example, resident registers, driver's license lists, central registers, directories of professional groups and companies, etc. Alternatively or additionally, the registration device 6 can also retrieve information from internal databases 34, e.g., in the form of CD-ROM drives. The

internal databases 34 can also constructed from the information obtained at registration. In this way, all registration processes can be logged and documented.

[0041]

Through the chip-card processing device 24 and the card-personalizing unit 27, authorization means can be processed in the form of chip cards, e.g., a digital signature card. The chip-card processing device 24 reads existing data, personalizes the pre-initialized chip cards, writes them with the necessary data, certificates, keys, etc., and outputs them.

[0042]

Figure 3 shows schematically the authentication system, in which the entire system is linked. A secure ID—ID1, ID2, ID4, ID6, and IDBi—is allocated to each of the "components" of the entire system comprising the higher-order authorization issuer 1, the lower-order authorization issuers 2i, the registration offices 4i, the registration devices 6i, and the authorized operators Bi. In addition, a secure ID—IDKi—can also be allocated to the individual hardware components Ki of the registration device 6. The secure ID can be, for example, an electronic key, a certificate, a PC dongle, etc.

[0043]

In the higher-order authorization issuer 1, a list of all ID2s of the authorization issuers 2 connected below this higher-order authorization issuer is controlled and managed. For communications between the higher-order authorization issuer 1 and one of the lower-order authorization issuers 2i, the two components are identified with reference to their corresponding ID—ID1 and ID2i. Likewise, a list of secure ID4i of the associated registration offices 4i is controlled for the lower-order authorization issuers 2i. For communications between the corresponding authorization issuers 2i and an allocated registration office 4i, the two components are again identified with reference to the secure ID2i or ID4i. Likewise, in the registration offices 4i, a list with the secure ID6i of the registration devices 6i connected to the corresponding registration office 4i is managed. In addition, the individual components Ki of the registration device 6i can also be provided with secure IDKi. In this way it is guaranteed that only "known" and "suitable" components Ki are coupled to the registration devices 6i or integrated into these devices.

[0044]

In addition, the operator Bi, who operates the registration devices 6i or their components Ki, must also be identified by a secure ID—IDBi. Alternatively, such a secure ID can be used

just to log into the corresponding component Ki or into the registration device 6i. The operator authorization IDBi can be given either by the authorization issuers 1, 2 or by the appropriate registration device 6i or the appropriate registration offices 4i.

[0045]

The appropriate secure IDs can be requested and exchanged for each communication between the individual components. Alternatively, the querying and exchange of the secure ID can be realized according to a certain time scheme or when certain events occur. The querying of the authorization ID IDBi of the operator Bi is performed at the start of the application "Identification/Registration," when the appropriate person logs in, or is repeated according to a certain time scheme or for every new registration process.

[0046]

The registration of a registrant or the operation of a registration device 6 can be realized both in an operator mode and also for non-critical applications in a self-operation mode. In self-operation mode, the registrant is guided through the individual registration steps by means of the screen, keyboard, and loudspeaker. In operator mode, an operator is present who performs the individual registration steps and certain verifications.

[0047]

The system according to the invention offers the following prerequisites in its preferred configuration for the secure identification and registration of persons:

1. The 4-eye principle is realized through a device that cannot be manipulated, with the core components of identification, authentication, and verification, and the auxiliary components of scanning and reading of documents, as well as detection of current biometric features (photo, signature, fingerprint, iris, etc.).

2. The secure device is a correspondingly secure environment (Figure 3). Here, the device should demand authenticated contact with an authorization issuer, such as a certified trust center, via a certified route. Therefore, the sale of such a device to persons who intend to make forgeries by issuing digital signature cards or other authorizations is harmless.

3. The device enables a preferably certified method for issuing authorization means.

4. There is only one responsible party, i.e., the process is performed in the presence of only one responsible person.

List of reference symbols

[0048]

1	Higher-order authorization issuer
2i	Lower-order authorization issuer
4i	Registration office
6i	Registration device
8	Controller
9	Monitor
10	Input means, such as keyboard, etc.
12	Printer
14	First document reader
15	Second document reader
16	Device for active capture of a biometric feature
18	Verification unit
20	Card payment unit
22	PIN input unit
23	Device for digitizing a signature
24	Chip card processing device
26	PIN output printer
27	Card-personalizing unit
28	DFÜ interface
30	Authentication unit
32	Uninterruptable power supply
34	External databases
36	Internal databases
Bi	Authorized operators
Ki	Components of 6i
ID1	Secure ID of 1
ID2i	Secure ID of 2i
ID4i	Secure ID of 4i
ID6i	Secure ID of 6i
IDKi	Secure ID of Ki

Claims

1. System for secure identification and registration of persons, especially for issuing personalized authorization means, such as a digital signature card, with:

at least one authorization issuer (1, 2) with an EDV system,

at least one registration office (4) with a registration device (6),

wherein the EDV systems of the authorization issuer (1, 2) and the registration device (6) of the registration offices (4) are connected to each other by means of a DFÜ and are linked in an authentication system (30, ID),

wherein the registration device (6) of the one or more registration offices (4) comprises at least one identification unit (14, 15, 16, 23), at least one output means (9, 12), at least one input means (9, 10), and a controller (8),

wherein the identification unit (14, 15, 16, 23) has a document reader (14, 15) for reading the documents identifying the registrant, such as, e.g., an official identification card, and means (16) for active capture of biometric data of the registrant.

2. System according to Claim 1, characterized by at least one verification unit (18), which (18) compares biometric features contained on the identifying documents detected by the document reader (14, 15) for agreement with the biometric features captured by the identification unit (14, 15, 16) and determines the result of the verification with reference to a preset identity likelihood.

3. System according to Claim 1 or 2, characterized by a verification unit (18), which tests the authenticity of the contents of the identifying and/or describing documents, in that the institution issuing the corresponding document is queried by DFÜ, [concerning] whether the appropriate document was actually issued with exactly these features and whether it is still valid.

4. System according to Claim 1, 2, or 3, characterized by at least one higher-order authorization issuer (1) with an EDV system.

5. System according to Claim 1, 2, 3, or 4, characterized in that programs and data for the secure identification and registration of persons, especially for issuing personalized authorizations, such as a digital signature card, are virtually or physically separated from other applications on the EDV systems of the authorization issuer (1, 2) and/or the registration devices (6) of the registration offices (4).

6. System according to Claim 1, 2, 3, 4, or 5, characterized in that the registration devices (6) of the registration offices (4) are used exclusively for the secure identification and registration of persons, especially for issuing personalized authorizations, such as a digital signature card.

7. System according to one of the preceding claims, characterized in that the identification unit (14, 15, 16, 23) of the registration offices (4) has a device for verifying the authenticity of the documents detected by the document reader (14).

8. System according to one of the preceding claims, characterized in that authorization issuers (1, 2) and/or registration offices (4) can be identified uniquely by means of a secure ID (ID1, ID2i, ID4i) in the form of an electronic key.

9. System according to Claim 8, characterized in that EDV systems or components of these systems for the authorization issuer (1, 2) and/or the registration devices (6) of the registration offices (4) can be identified uniquely by means of a secure ID (ID6i, IDKi) in the form of an electronic key.

10. System according to Claim 8 or 9, characterized in that the secure ID is an electronic certificate and/or a digital signature and/or a hardware component.

11. System according to one of the preceding Claims 8-10, characterized in that the issuing of the secure ID (ID1, ID2i) of the authorization issuer (1, 2) is performed by the higher-order authorization issuer (1).

12. System according to one of the preceding Claims 8-11, characterized in that the issuing of the secure ID (ID6i) of the registration offices (6) is performed by the authorization issuer (2).

13. System according to one of the preceding Claims 8-12, characterized in that the secure ID is verified by the issuing office periodically or when certain events occur.

14. System according to one of the preceding Claims 8-13, characterized in that the registration device (6i) of the registration offices (4) is functional only with the presence of a secure ID of the corresponding registration office (4) and a secure ID of the associated authorization issuer (1, 2).

15. System according to one of the preceding claims, characterized in that the operation of the EDV systems and/or the registration devices (6) is possible only by authorized persons (Bi) with a corresponding secure ID (IDBi).

16. Registration device, especially for a system according to one of Claims 1-15, with at least one identification unit (14, 15, 16, 23), at least one verification unit (18), at least one output means (9, 12), at least one input means (9, 19), and a controller (8), wherein the identification unit (14, 15, 16, 23) has a document reader (14, 15) for reading documents identifying the registrant, such as, e.g., an official identification card, and means (16) for active capture of biometric data of the registrant, and

wherein the verification unit (18) compares biometric features contained on the identifying documents captured by the document reader (14, 15) for agreement with the biometric features captured by the identification unit (14, 15, 16, 23) and determines the result of the verification with reference to a preset identity likelihood.

17. Registration device according to Claim 16, characterized by another document reader (15).

18. Registration device according to Claim 16 or 17, characterized by a device (20) for payment, especially by an EFTPOS terminal and/or an interface device (28) for accessing internal and/or external databases and registers (34, 36).

19. Registration device according to one of Claims 16-18, characterized by a processing device (24, 27) for authorization means, especially in the form of chip cards.

20. Registration device according to one of Claims 16-19, characterized in that the identification unit (14, 15, 16, 23) comprises a device (23) for detecting the dynamic response of a biometric feature.

21. Method for operating a system for secure identification and registration of persons for issuing personalized authorization means according to one of the preceding claims with the processing steps:

a) inserting a document identifying the registrant into the document reader (14, 15), wherein the identifying document contains at least one biometric feature of the registrant;

b) reading the personal data from the identifying document;

c) transferring of the one or more biometric features of the registrant from the identifying document;

d) actively detecting of at least one biometric feature of the registrant, wherein at least one of the actively detected biometric features has been transferred in step c) from the identifying document;

e) verifying of data from the identifying document with the actively detected data for agreement;

f) determining the identity using the agreement in step e) with a certain likelihood; and

g) releasing of the desired personalized authorization means for issuance.

22. Method according to Claim 21, characterized by the additional processing step: verifying the physical authenticity of the identifying document.

23. Method according to one of Claims 21 or 22, characterized by the additional processing step: reading of at least one additional document describing the person to be identified as the registrant.

24. Method according to one of Claims 21-23, characterized in that attributes of the registrant, such as powers of attorney, authorizations, etc., are read from the additional document.

25. Method according to one of Claims 21-24, characterized by the additional processing step:

verifying the authenticity of the contents of the identifying document, in that the institution issuing the identifying document is queried by DFÜ [concerning] whether the corresponding identifying document has actually been issued with exactly these features and is still valid.

26. Method according to one of Claims 21-25, characterized by the additional processing step:

selection of the desired registration or of the desired authorization means at the beginning of the registration.

27. Method according to one of Claims 21-26, characterized by the additional processing step:

expanding the personalized data from existing data sets and/or through dialog-guided questioning of the registrant.

28. Method according to one of Claims 21-27, characterized in that the detected data, features, and other information are displayed on a display device.

29. Method according to one of Claims 21-28, characterized in that the detected data, features, and other information are printed out.

30. Method according to one of Claims 21-29, characterized in that the detected data, features, and other information are displayed in the form of a request and/or printed out.

31. Method according to one of Claims 21-30, characterized in that the registration process is verified by the registrant by means of a signature; that the provided signature is compared with the signature on the identifying document; and that with sufficient agreement, the release of the desired registration is realized.

32. Method according to one of Claims 21-31 for issuing a digital signature card, characterized by the additional processing steps:

A) reading the PSE data necessary for producing and processing the certificate by the authorization issuer from a pre-initialized chip card in a correspondingly highly certified card reader/writer;

B) exporting the detected data of the registrant into a software program corresponding to the legal regulations;

C) allocation of the data of the registrant to the PSE data;

D) compiling the data needed by the authorization issuer and display on a legally conforming display device;

E) signing, encryption, and transfer of these data to the authorization issuer;

F) processing by the authorization issuer and transmittal of the data needed for creating the signature card, such as a certificate or release code, digitally signed and encrypted, to the registration office;

G) decryption and verifying of the data transmitted by the authorization issuer;

H) if the verification in step G) is positive: personalization and transmission of the required data with certificate to the pre-initialized chip card;

I) instruction of the registrant according to legal regulations; and

J) printout of preferably two confirmations of the successful instruction, and confirmation of receipt of the digital signature card.

33. Method according to Claim 32, characterized by the additional processing steps: verifying of the uniqueness of the key contained in the PSE data of the pre-initialized chip card by the authorization issuer.

34. Method according to Claim 32 or 33, characterized in that in step E), the verification result is also transmitted to the authorization issuer.

35. Method according to one of Claims 32-34, characterized in that the digital signature card is output only when the registrant changes the PIN of the digital signature card.

36. Method according to one of Claims 32-35, characterized in that the instruction in step I) is realized in the form of a programmed, dialog-guided training with a test, and that the digital signature card is activated only when the registrant has successfully completed the training program and test.

37. Method according to one of Claims 21-36, characterized in that an activation report is generated to a third person, who has allotted authorizations, especially power of representation, for the corresponding registrant and the corresponding authorization means, wherein the information on the authorizations is stored on the authorization means.

38. Method according to one of Claims 21-37, characterized in that the registration ends after completion of the registration or after a certain time period has elapsed.

39. Method according to one of Claims 21-38, characterized in that the registration offices log all registration processes, in that the logs with the associated personalized data and requested documents are transmitted according to a certain scheme to the authorization issuer, and in that the authorization issuer verifies the logs, documents, and data in terms of legibility and completeness.

40. Method according to one of Claims 21-39, characterized in that the data and documents obtained and evaluated in the registration offices are deleted according to a certain time scheme.

41. Method according to one of Claims 21-40, characterized in that the data and documents obtained and evaluated in the registration offices are deleted after deletion release by the authorization issuer.

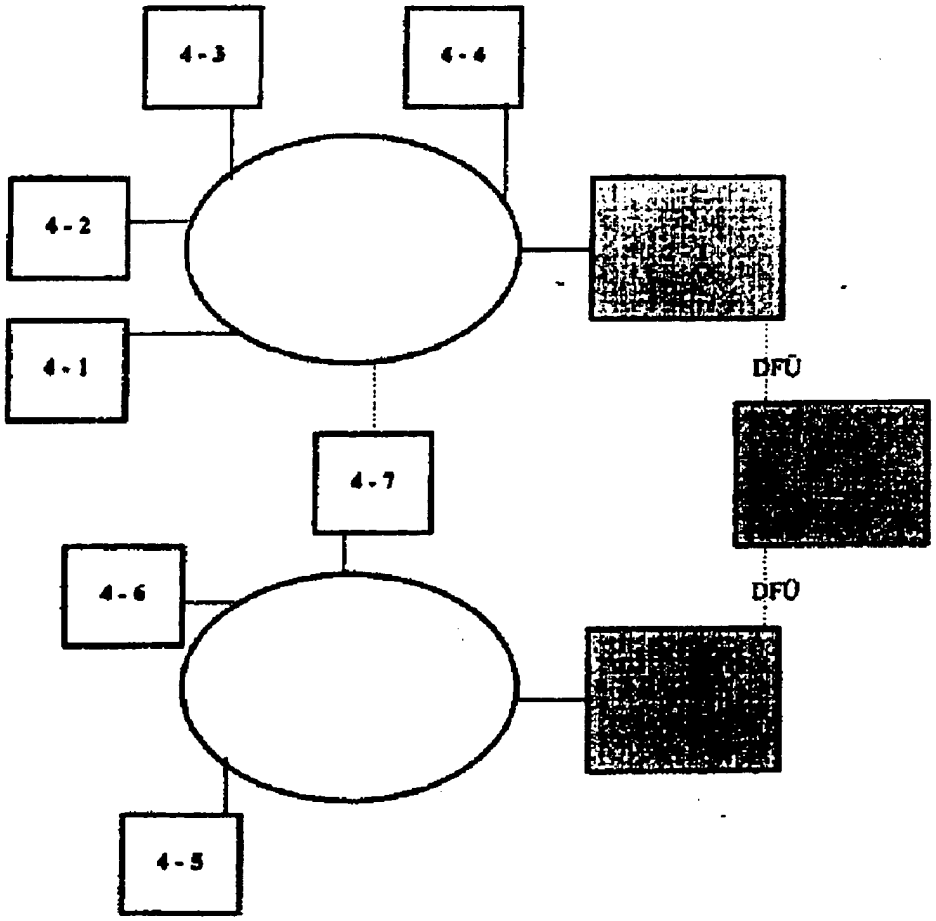


Figure 1

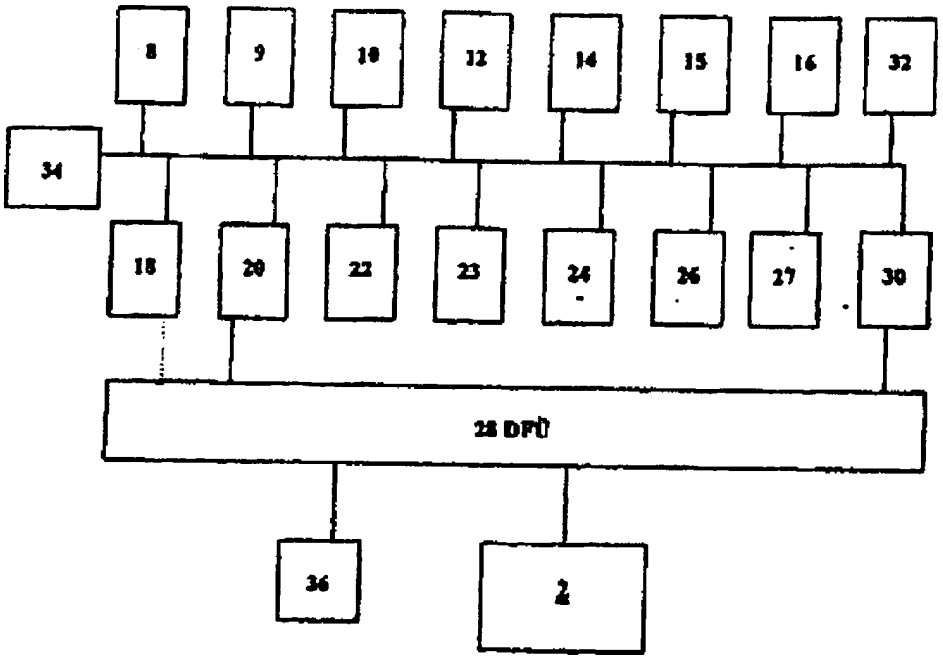


Figure 2

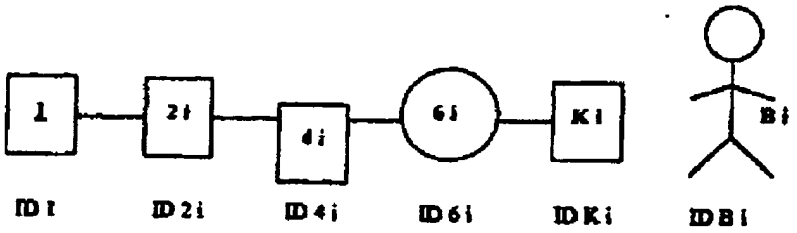


Figure 3

System and method for secure identification and registration of persons, particularly for the issue of personalized authentication means such as digital signature cards as well as a registration device adapted for such a system

Patent number:	EP0999528
Publication date:	2000-05-10
Inventor:	WAGNER INGVAR (DE)
Applicant:	ELSDALE LIMITED (GB)
Classification:	
- international:	G07F7/10; G06K19/07
- european:	
Application number:	EP19990122157 19991105
Priority number(s):	DE19981051074 19981105

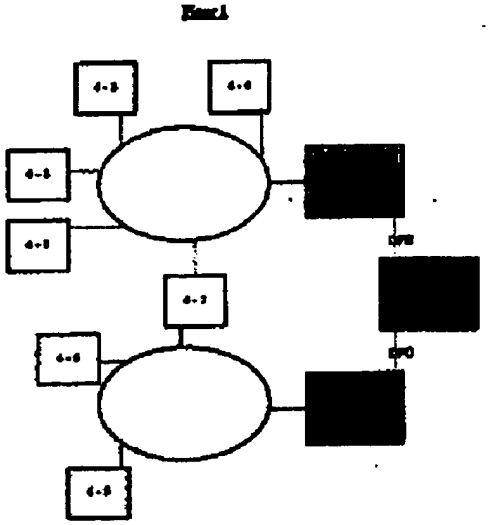
Also published as:
- EP0999528 (A3)
- DE19851074 (A1)

Cited documents:
- WO9828721
- US5717776
- EP0950999
- US4995086
- US5280527

Report a data error here

Abstract of **EP0999528**

Person specific data is read from official identifying document at registration location. Document contains at least one biometric characteristic of the person, e.g. photo, signature, finger print etc. Biometric characteristic is also detected on the spot from the person and compared with data from identifying document. A higher order authorization provider (1) is connected by remote data exchange with trust centers (2-1,2-2). Each trust center is connected with registration locations (4-1 - 4-7). Each location has computer with document readers and device for on the spot detection of biometric characteristic of person to be registered. Person specific data is read from official identification for verification. Registration can be self-service or operator controlled. Independent claim is included for procedure to issue signature card.



Data supplied from the *esp@cenet* database - Worldwide

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 999 528 A2

(12) EUROPÄISCHE PATENTANMELDUNG

(43) Veröffentlichungstag:
10.05.2000 Patentblatt 2000/19

(51) Int. Cl.[7]: G07F 7/10, G06K 19/07

(21) Anmeldenummer: 99122157.3

(22) Anmeldetag: 05.11.1999

(84) Benannte Vertragsstaaten:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Benannte Erstreckungsstaaten:
AL LT LV MK RO SI

(30) Priorität: 05.11.1998 DE 19851074

(71) Anmelder: Eladale Limited
St. Helier, Jersey (GB)

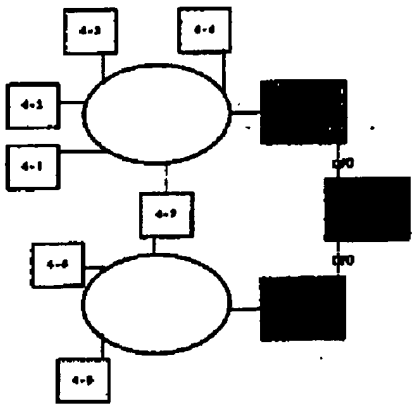
(72) Erfinder: Wagner, Ingvar
63128 Dietzenbach (DE)

(74) Vertreter:
Winter, Brandl & Partner
Patent- und Rechtsanwaltskanzlei
Alois-Steinecker-Strasse 22
85354 Freising (DE)

(54) System und Verfahren zur sicheren Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungsmitteln wie einer digitalen Signaturkarte sowie eine für ein solches System geeignete Registriereinrichtung

(57) Es wird ein System in einem Verfahren zur sicheren Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungsmitteln wie einer digitalen Signaturkarte angegeben. Die sichere Registrierung erfolgt in einem System bestehend aus einem Berechtigungsherausgeber, zum Beispiel einem Trust Center, und wenigstens einer Registrierungsstelle, wobei Berechtigungsherausgeber und Registrierungsstelle in ein Authentifikationssystem eingebunden sind das sicherstellt, daß nur von dem Berechtigungsherausgeber berechtigte Registrierungsstellen die Registrierung vornehmen können. Dies wird dadurch erreicht, daß personenbezogene Daten von einem die zu registrierende Person identifizierenden Dokument eingelesen werden, wobei das zu identifizierende Dokument wenigstens ein biometrisches Merkmal der Person enthält. Das von dem identifizierenden Dokument übernommene biometrische Merkmal wird auch vor Ort von der anwesenden Person übernommen beziehungsweise gemacht. Eine Verifikationseinheit vergleicht die unmittelbar vor Ort erfassten Daten mit denen von dem identifizierenden Dokument erfassten Daten und stellt mit einer gewissen Wahrscheinlichkeit fest, ob es sich bei der eine Registrierung nachsuchenden Person auch tatsächlich um die Person handelt, die sie vorgibt zu sein.

Fig. 1



EP 0 999 528 A2

Beschreibung

[0001] Die Erfindung betrifft ein System und ein Verfahren zur sicheren Identifikation und der Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungsmitteln wie einer digitalen Signaturkarte sowie eine für ein solches System geeignet Registriereinrichtung.

[0002] Das Gesetz zur digitalen Signatur (Signaturgesetz) regelt die Rahmenbedienungen nach denen digitale Signaturen, Zertifikate und Zeitstempel ausgegeben werden. Es besteht daher ein Bedarf an gesetzeskonformen Einrichtungen, Systemen und Verfahren zur sicheren Identifikation und Registrierung von Personen, so daß gewährleistet ist, daß Berechtigungen wie digitale Signaturkarten nur an sicher identifizierte Personen herausgegeben werden. Da bei Ausgabe einer Signaturkarte an eine unberechtigte Person Haftungsfragen für Registrierungsstellen und Trust Center (Berechtigungsherausgeber) auftreten, besteht Bedarf für eine sicheres Ausgabeverfahren und -system. Die gesetzlichen Bestimmungen allein geben diese Sicherheit noch nicht.

[0003] Aus der WO-A 98/28721 ist ein Gerät bekannt, welches Personendaten unter anderen mit einem Ausweisleser erfaßt und zur Ausgabe von weiteren personenbezogenen Dokumenten verarbeitet. Hierbei ist jedoch nicht sichergestellt, daß die erfaßten Personendaten tatsächlich die Personendaten der anwesenden Person sind. Es könnte z. B. ein amtlicher Ausweis gelesen werden der nicht zu der anwesenden Person gehört.

[0004] Es ist daher Aufgabe der vorliegenden Erfindung ein System und ein Verfahren zur sicheren Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungsmitteln, wie einer digitalen Signaturkarte anzugeben, bei denen gewährleistet ist, daß das Berechtigungsmittel bzw. die Freigabe zur Herausgabe dieses Berechtigungsmittel nur an eine sicher identifizierte Person erteilt wird. Weiter ist es Aufgabe der vorliegenden Erfindung eine für das System geeignete Registriereinrichtung anzugeben.

[0005] Die Lösung dieser Aufgabe erfolgt durch die Merkmale der Ansprüche 1, 16 bzw. 21.

[0006] Die sichere Registrierung erfolgt in einem System bestehend aus einem Berechtigungsherausgeber, bei der Herausgabe von digitalen Signaturkarten einem sogenannten Trust Center, und wenigstens einer Registrierungsstelle, wobei Berechtigungsherausgeber und Registrierungsstelle(n) in ein Authentifikationssystem eingebunden sind, das sicher stellt, daß nur von dem Berechtigungsherausgeber berechtigte Registrierungsstellen die Registrierung vornehmen können. Damit wird verhindert, daß "falsche" Berechtigungsmittel in Umlauf geraten. Die Registrierungsstellen umfassen hierbei erfindungsgemäße Registriereinrichtungen mit denen zuverlässig ermittelt werden kann, ob eine um eine Registrierung nachsuchende Person tatsächlich diejenige Person ist, die sie vorgibt zu sein. Dies wird dadurch erreicht, daß personenbezogene Daten von einem die zu registrierende Person identifizierende Dokument eingelesen werden, wobei das zu identifizierende Dokument wenigstens ein biometrische Merkmal der Person, wie z. B. ein Paßfoto, eine Unterschrift, einen Fingerabdruck oder dgl. enthält. Das von dem identifizierende Dokument übernommene biometrische Merkmal wird auch vor Ort von der anwesenden Person übernommen, indem z. B. ein Foto der anwesenden Person gemacht wird oder indem die anwesende Person eine Unterschriftsprobe gibt. Gemäß einer vorteilhaften Ausprägung der Erfindung vergleicht eine Verifikationseinheit die unmittelbar vor Ort erfaßten Daten mit dem von dem identifizierenden Dokument erfaßten Daten und stellt mit einer gewissen Wahrscheinlichkeit fest, ob es sich bei der um einer Registrierung nachsuchenden Person auch tatsächlich um die Person handelt, die sie vorgibt zu sein. Die Identität der um einer Registrierung nachsuchenden Person wird mit einer bestimmten Wahrscheinlichkeit festgestellt, wobei einstellbar ist, mit welcher Wahrscheinlichkeit die Identität festgestellt werden muß, um die Herausgabe eines Berechtigungsmittels freizugeben.

[0007] Gemäß einer vorteilhaften Ausgestaltung der Erfindung ist dem Berechtigungsherausgebern ein übergeordneter Berechtigungsherausgeber (Root) zugeordnet, der ebenfalls in das Authentifikationssystem eingebunden wird.

[0008] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung sind die Programme und Daten für die erfindungsgemäße Anwendung auf den EDV-Anlagen der Berechtigungsherausgeber und der Registrierungsstellen physisch oder virtuell von anderen Anwendungen getrennt. Alternative können die EDV-Anlagen mit ihren Komponenten auch ausschließlich für die sichere Identifikation und Registrierung von Personen für die Herausgabe von Berechtigungsmitteln genutzt werden. Hierdurch wird die Möglichkeit von Manipulationen verringert.

[0009] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung überprüft der Dokumentenleser in der Identifikationseinheit die Echtheit des eingelesenen Dokuments. Diese Prüfung kann sowohl die physische Echtheit durch Erfassung von Wasserzeichen, Sicherungsfäden, Papierart usw., als auch die Prüfung der inhaltlichen Echtheit durch Abgleich mit externen Datenbanken, etc. umfassen.

[0010] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung wird das Authentifikationssystem dadurch verwirklicht, daß sowohl die Berechtigungsherausgeber als auch die Registrierungsstellen mittels einer sicheren ID, z. B. in Form eines elektronischen Schlüssels, eindeutig identifizierbar sind. Das heißt, die einzelnen Komponenten des Systems sind mit einer sicheren ID in Form eines elektronischen Zertifikats, in Form einer digitalen Signaturkarte etc. eindeutig identifiziert,

wodurch Manipulationen erschwert werden. Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung sind auch die einzelnen Komponenten der Berechtigungsherausgeber und der Registrierungsstellen mit individuellen sicheren IDs ausgestattet. Auf diese Weise kann sicher verhindert werden, daß sich externe Komponenten in dieses System mit sicheren IDs einschalten, so daß Manipulationen nahezu ausgeschlossen sind.

[0011] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die sichere ID der Berechtigungsherausgeber durch den übergeordneten Berechtigungsherausgeber erteilt und die sichere ID der Registrierungsstellen erfolgt durch die zugeordneten Berechtigungsherausgeber. Auch hierdurch wird die Manipulationssicherheit erhöht.

[0012] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung werden die sicheren IDs, der Berechtigungsherausgeber, der Registrierungsstellen, sowie der einzelnen Komponenten periodisch oder bei bestimmten Ereignissen überprüft, so daß immer gewährleistet ist, daß nur "berechtigte" Komponenten und Stellen in das erfindungsgemäße System eingebunden sind.

[0013] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung ist die Registriereinrichtung nur funktionsfähig, d. h. es können nur Registrierungen vorgenommen werden, wenn sowohl die sichere ID der jeweiligen Registrierungsstelle als auch die sichere ID des zugehörigen Berechtigungsherausgebers vorliegt und als richtig erkannt worden ist. Auch hierdurch wird die Manipulationssicherheit erhöht.

[0014] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung lassen sich die einzelnen Komponenten der EDV-Anlagen bzw. der Registriereinrichtungen nur durch "berechtigte" Personen mit einer sicheren ID aktivieren. Das heißt, jede Bedienungsperson muß beispielsweise ihre persönliche digitale Signaturkarte in das Gerät einschieben und nur wenn die jeweilige Hardwarekomponente die durch die digitale Signaturkarte identifizierte Person als "berechtigte" Person erkennt, läßt sich die jeweilige Hardwarekomponente aktivieren bzw. das Anwendungsprogramm für die Registrierung und Identifikation der Personen aufrufen. Anstelle einer digitalen Signaturkarte kann auch ein spezieller elektronischer Schlüssel, Passwörter, biometrische Merkmale, etc. verwendet werden. Auch hierdurch wird die Manipulationssicherheit weiter erhöht.

[0015] Gemäß einer weiteren vorteilhaften Ausgestaltung ersparen elektronische Schnittstellen zu Melderegistern dem "Kunden" - der zu registrierenden Person - den Weg zur Gemeinde, Wohnsitzbestätigungen können online eingeholt werden. Die elektronischen Schnittstellen zu externen und internen Registern und Datenbanken können generell zum Abgleich von Daten, Beschaffung benötigter Daten und für Plausibilitätsprüfungen verwendet werden. Durch die Möglichkeit der bargeldlosen Zahlung mittels EFT-POS werden Kasse und Buchhaltung entlastet.

[0016] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung umfaßt die Registriereinrichtung eine Chipkarten-Bearbeitungseinrichtung mittels der die notwendigen Daten und Informationen in Berechtigungsmittel in Form von Chipkarten ein- bzw. aufgebracht werden. Dies gilt insbesondere für die Ausgabe von digitalen Signaturkarten. Damit können Berechtigungsmittel in Form von Karten auf der Oberfläche oder in der Karte mit Merkmalen versehen werden. So kann der Name des Berechtigten aufgedruckt sein, es können Merkmale in unsichtbarer Schrift aufgedruckt werden oder das Foto des Berechtigen wird auf das Berechtigungsmittel aufgedruckt.

[0017] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung umfassen die Identifikationseinheiten der Registriereinrichtungen auch eine Einrichtung zur Erfassung der Dynamik eines biometrischen Merkmals. Damit kann beispielsweise die Schreibgeschwindigkeit und die Druckverteilung bei der Unterschrift erfaßt und überprüft werden. Hierdurch kann die Wahrscheinlichkeit mit der die Identität einer Person festgestellt wird weiter erhöht werden.

[0018] Mit dem erfindungsgemäßen Verfahren nach Anspruch 21 kann die Identität einer um einer Registrierung nachsuchenden Person sicher festgestellt werden.

[0019] Gemäß einer vorteilhaften Ausgestaltung der Erfindung kann zu Beginn der Registrierung ausgewählt werden, welches Berechtigungsmittel, z. B. digitale Signaturkarte, gewünscht wird. Auf diese Weise lassen sich mit ein und derselben Registriereinrichtung verschiedene Berechtigungsmittel ausgeben bzw. die Freigabe für die Ausgabe erteilen.

[0020] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die Sicherheit der Identifikation dadurch erhöht, daß neben personenbezogenen Daten von einem identifizierenden Dokument auch personenbezogene Daten von internen und externen Datenbanken, wie z. B. einem Einwohnermelderegister, Führerscheinlisten, einem Zentralregister, CD-ROM, etc. hinzugezogen und auf Übereinstimmung geprüft werden. Außerdem ist auch eine dialoggeführte Rückfrage bei der zu registrierenden Person möglich. Weiter können benötigte Angaben, Merkmale und Attribute der zu registrierenden Person von weiteren die zu registrierende Person beschreibenden Dokumenten eingelesen und verarbeitet werden.

[0021] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung lassen sich die erhobenen Daten anzeigen und/oder ausdrucken. Dies kann lediglich zur Information oder in Form eines Antrags erfolgen, der dann auch gleich unterzeichnet werden kann.

[0022] Das erfindungsgemäße System eignet sich insbesondere für die Ausgabe einer digitalen Signaturkarte gemäß Anspruch 32. Hierbei wird zunächst die Person, die um eine digitale Signaturkarte nachfragt gemäß dem erfindungsgemäßen Verfahren sicher iden-

tifiziert. Zusätzlich werden PSE-Daten von einer vorinitialisierten Chipkarte ausgelesen und an ein Softwareprogramm übergeben. Durch die Software werden die personenbezogenen Daten des sicher identifizierten Antragstellers mit den PSE-Daten kombiniert und die für die Herausgabe der digitalen Signaturkarte benötigten Daten werden auf einer gesetzeskonformen Anzeige angezeigt. Danach werden die relevanten Daten signiert, verschlüsselt und an den Berechtigungsherausgeber übertragen. Nach Überprüfung beim Berechtigungsherausgeber wird das zugehörige Zertifikat digital signiert und verschlüsselt an die Registrierungsstelle übertragen. In der Registrierungsstelle werden die übertragenen Daten entschlüsselt und wiederum überprüft und im Falle eines positiven Ergebnisses der Überprüfung bzw. der Freigabe durch den Berechtigungsherausgeber werden die erforderlichen Daten mit dem Zertifikat auf die vorinitialisierte Chipkarte übertragen und diese personalisiert. Dann erfolgt die vom Gesetz vorgeschriebene Belehrung und der Ausdruck einer Bestätigung über die erfolgte Belehrung und dem Erhalt der digitalen Signaturkarte.

[0023] Gemäß einer vorteilhaften Ausgestaltung der Erfindung wird die Einmaligkeit des in dem PSE-Daten der vorinitialisierten Chipkarte enthaltenen Schlüssels durch den Berechtigungsherausgeber entweder bei der Übergabe des Zertifikats oder vorab überprüft.

[0024] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung erfolgt die Belehrung bei Ausgabe der digitalen Signaturkarte mittels einer programmierten, dialoggeführten Unterweisung mit anschließendem Test. Nur wenn der Test erfolgreich abgeschlossen wird, wird die Signaturkarte aktiviert. Auf diese Weise wird den gesetzlichen Anforderungen hinsichtlich der Belehrung Rechnung getragen und gleichzeitig wird der Personalaufwand für diese gesetzlich vorgeschriebene Belehrung minimiert.

[0025] Gemäß einer weiteren vorteilhaften Ausgestaltung des erfindungsgemäßen Verfahrens wird bei Ausgabe eines Berechtigungsmittels, z. B. in Form einer digitalen Signaturkarte oder bei der Freigabe zur Ausgabe eines Berechtigungsmittels eine Mitteilung an eine dritte Person erzeugt. Dies ist dann sinnvoll, wenn diese dritte Person die zu registrierende Person beauftragt oder bevollmächtigt hat, in das jeweilige Berechtigungsmittel weitere Berechtigungen wie Vollmachten eintragen zu lassen. Auf diese Weise kann z. B. Prokura einer Firma elektronisch erteilt werden und die Prokura erteilende Institution oder Person wird davon in Kenntnis gesetzt.

[0026] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung wird die Registrierung nach erfolgreichem Abschluß einer Registrierung selbst tätig beendet, d. h. das Gerät bzw. die Registriereinrichtung deaktiviert sich selbst oder die Registrierung wird nach einer bestimmten Zeitdauer automatisch abgebrochen, da bei Überschreiten einer maximalen Dauer für eine Registrierung ein Manipulationsversuch angenommen wird.

[0027] Gemäß weiterer vorteilhaften Ausgestaltungen wird jeder Registrierungsvorgang und auch die Kommunikation zwischen den einzelnen Komponenten des erfindungsgemäßen Systems protokolliert, so daß Manipulationen oder Unregelmäßigkeiten sicher nachgewiesen und bestimmten Personen zugeordnet werden können. Zusätzlich werden die Protokolle und Daten nach einem bestimmten Schema an den zugehörigen Berechtigungsherausgeber übermittelt, der sie auf Vollständigkeit und Richtigkeit überprüft oder um eventuelle Manipulationen festzustellen und sie anschließend in eine elektronische Ablage überführt. Die gesamte Archivierung von Papierdokumenten kann damit entfallen. Ein erheblicher Vorteil, sowohl für die Registrierungsstellen als auch für die Berechtigungsherausgeber. Die elektronische Archivierung und Fehlerprüfung gehen Hand in Hand.

[0028] Gemäß einer weiteren vorteilhaften Ausgestaltung der Erfindung werden die erhobenen Daten und Protokolle bei der Registrierungsstelle nach einem bestimmten Schema gelöscht, wobei die Löschungsfreigabe vorzugsweise durch den zugehörigen Berechtigungsherausgeber erfolgt. Auf diese Weise soll Datenschutz gewährleistet und Manipulation mit den erhobenen Daten ausgeschlossen werden.

[0029] Die übrigen Unteransprüche beziehen sich auf weitere vorteilhafte Ausgestaltungen der Erfindung.

[0030] Durch die Zuweisung von sicheren IDs und deren Austausch und Überprüfung werden Manipulationen und Unregelmäßigkeiten nahezu vollständig ausgeschlossen, zumindest aber können diese einem Verantwortlichen beweisträchtig zugeordnet werden. Darüber hinaus macht die Verwendung von sicheren IDs die zugeordneten Geräte ohne diese sicheren IDs nutzlos. Im Extremfall ist eine derartige Hardware-Komponente nur funktionsfähig, wenn die sichere ID des Berechtigungsherausgebers, die sichere ID der jeweiligen Registrierungsstelle, die sichere ID der jeweiligen Komponente und die sichere ID eines berechtigten Benutzers vorliegt. Damit besteht selbst bei Diebstahl oder bei Weiterveräußerung einer derartigen Komponente an unberechtigte Dritte kein Sicherheitsrisiko.

[0031] Die Ausgabe von Signaturkarten ist neu und noch lange kein Routinevorgang, der mit entsprechender Perfektion und Qualität durchgeführt wird. Es werden anfangs "Kinderkrankheiten" auftreten. Die mangels Masse fehlende Erfahrung und notwendige Lernprozesse können hohe Fehlerraten, Unsicherheiten bei den "Verkäufern" und Mißstimmungen bei den neuen "Kunden" hervorrufen. Das ist Gift für die Markteinführung. Durch das erfindungsgemäße System wird die Qualitätssicherung bei der Registrierung und der Kartenausgabe nach dem Signaturgesetz erleichtert und übliche Anlaufschwierigkeiten werden gemildert. Durch die weitgehende Automatisierung, jedoch mit Eingriffsmöglichkeit von Bedienungspersonal, wird eine

gleichbleibend hohe Qualität sichergestellt, was bei Vorgängen, die von Erfüllungsgehilfen nur gelegentlich (z. B. 1 bis 2 mal täglich) bearbeitet werden, nur sehr schwer zu erreichen ist.

[0032] Das erfindungsgemäße System und Verfahren ist wirtschaftlicher als das rein manuelle Verfahren. Die vorwiegend manuellen und Papier gestützten Verfahren sind personalintensiv und deshalb teuer. Dazu kommen Medienbrüche, die teilweise Doppelarbeit, immer aber Fehlerquellen darstellen. Die Kosten für die Qualitätssicherung sind deshalb hoch. Je nach Vorgaben ist das System nach der vorliegenden Erfindung ab etwa 35 Registrierungen/Anträgen/Karten pro Monat günstiger als manuale Verfahren. Die Überlegenheit gründet auf den verkürzten Bearbeitungszeiten in den Registrierungsstellen und bei den Berechtigungsherausgebern (TrustCentern).

[0033] Die erfindungsgemäße Registrierung und Kartenausgabe hat daher gegenüber herkömmlichen Verfahren folgende Vorteile:

- die Wirtschaftlichkeit gegenüber anderen, insbesondere manuellen Verfahren;
- die Bequemlichkeit der Registrierung im Vergleich zu anderen Verfahren;
- Erfüllung von künftigen Haftungsregeln für Berechtigungsherausgeber und deren Erfüllungsgehilfen;

[0034] Für die "Verkäufer" wird eine hohe Ablaufsicherheit gewährleistet, dem "Kunden" wird Bequemlichkeit geboten und bei den Berechtigungsherausgebern schlagen Arbeitserleichterungen, Minderung der Haftungsrisiken und Senkung der Kosten der Registrierung zu Buche.

[0035] Weitere Einzelheiten, Merkmale und Vorteile der Erfindung ergeben sich aus der nachfolgenden Beschreiben einer beispielhaften Ausführungsform der Erfindung anhand der Zeichnung.

[0036] Es zeigt

Fig. 1 eine schematische Darstellung des Gesamtsystems;

Fig. 2 eine schematische Darstellung einer Registriereinrichtung in einer Registrierungsstelle; und

Fig. 3 eine schematische Darstellung zur Erläuterung des Authentifikationssystems mit sicheren IDs.

[0037] Figur 1 zeigt eine schematische Darstellung des erfindungsgemäßen Systems mit einem übergeordneten Berechtigungsherausgeber 1, der mittels Datenfernübertragung (DFÜ) mit zwei nachgeordneten Berechtigungsherausgebern - auch Trust Center genannt - 2-1 und 2-2 verbunden werden kann (strichliert gezeichnet). Der erste Berechtigungsherausgeber 2-1 ist mittels DFÜ mit einer Mehrzahl von Registrierungsstellen 4-1 bis 4-4 verbunden. Der zweite Berechtigungsherausgeber bzw. das zweite Trust Center 2-2 ist ebenfalls mittels DFÜ mit zwei Registrierungsstellen 4-5 bis 4-7 verbunden. Die einzelnen Registrierungsstellen können auch mit mehreren Berechtigungsherausgebern 2i verbunden sein. Dies ist für die Registrierungsstelle 4-7 beispielhaft durch die strichlierte Verbindung gezeigt.

[0038] Jede der Registrierungsstellen 4 umfaßt wiederum wenigstens eine Registriereinrichtung 6, deren Aufbau schematisch in Figur 2 dargestellt ist Die Registriereinrichtung 6 umfaßt eine Steuereinheit 8, z. B. in Form eines PCs, einen Bildschirm 9, ein Eingabemittel 10 in Form einer Tastatur oder dgl., ein Ausgabemittel in Form eines Druckers 12, einen ersten Dokumentenleser 14, einem zweiten Dokumentenleser 15 und eine Einrichtung 16 zur Vor-Ort-Erfassung eines biometrischen Merkmals der zu registrierenden Person. Die Registriereinrichtung 6 umfaßt desweiteren eine Verifikationseinheit 18, eine Kartenbezahlungseinheit 20 mit Modem, eine PIN-Eingabeeinrichtung 22, eine Einrichtung 23 zur Digitalisierung einer Unterschrift, eine Chipkarten-Beschriftungseinrichtung 24, einen PIN-Ausgabedrucker 26, eine Kartenpersonalisiereinheit 27, eine DFÜ-Schnittstelle 28, eine Authentifizierungseinheit 30 und eine unterbrechungsfreie Stromversorgung 32.

[0039] Der erste Dokumentenleser 14 dient zum Einlesen von personenbezogenen Daten von amtlichen Ausweisen und umfaßt auch eine Einheit zum Überprüfen der Echtheit der eingelesenen Dokumente. Darüber hinaus erfaßt der Dokumentenleser auch Fotos, Unterschriften, Fingerabdrücke, Fotos der Iris usw. von identifizierenden Dokumenten, die dann in der Verifikationseinheit 18 weiterverarbeitet werden. Der zweite Dokumentenleser 15 ist für andere und nichtamtliche Dokumente vorgesehen. Die Einrichtung 16 kann eine elektronische Kamera, ein Gerät zur Aufnahme von Fingerabdrücken, ein Gerät zur Aufnahme der Iris oder ähnliches sein. Die Einrichtung 23 zur Digitalisierung einer Unterschrift kann sowohl zur aktuellen Erfassung des biometrischen Merkmals "Unterschrift" verwendet werden als auch zum Unterzeichnen eines Antrags auf Herausgabe einer digitalen Signaturkarte. Dabei wird die Unterschrift gleichzeitig elektronisch aufgezeichnet und den elektronischen Dokumenten als Bild und digital und digital hinzugefügt Über die PIN-Eingabeeinheit 22 kann sich eine berechtigte Bedienungsperson BI und die zu registrierende Person über eine ihr bereits zugeordnete PIN identifizieren. Die PIN-Eingabeeinheit stellt eine Komponente eines auf Wissen und Lernen basierenden Identifikationssystem dar.

[0040] Über die Authentifizierungseinheit 30 und die DFÜ-Schnittstelle 28 ist die Registriereinrichtung 6 mit dem zugehörigen Berechtigungsherausgeber 2 verbindbar. Über die DFÜ-Schnittstelle 28 ist die Registriereinrichtung 6 auch mit externen Datenbanken 36 verbindbar, bei dem es sich beispielsweise um ein Ein-

wohnermelderegister, Führerscheinstellen, Zentralregister, Verzeichnisse von Berufsständen und Unternehmern usw. handelt. Alternativ oder zusätzlich kann die Registriereinrichtung 6 auch aus internen Datenbanken34, z. B. in Form von CD-ROM-Laufwerken, Informationen abrufen. Die internen Datenbanken 34 können auch durch die Information, die bei der Registrierung anfällt aufgebaut werden. Alle Registrierungsvorgänge lassen sich darauf protokollieren und dokumentieren.

[0041] Durch die Chipkarten-Bearbeitungseinrichtung 24 und die Kartenpersonalisiereinheit 27 können Berechtigungsmittel in Form von Chipkarten, z. B. eine digitale Signaturkarte bearbeitet werden. Die Chipkarten-Bearbeitungseinrichtung 24 liest vorhanden Daten, personalisiert die vorinitialisierten Chip-Karten, beschreibt sie mit den nötigen Daten, Zertifikaten, Schlüsseln, etc. und gibt sie aus.

[0042] Figur 3 zeigt schematisch das Authentifikationssystem in das das Gesamtsystem eingebunden ist. Jeder der "Komponenten" des Gesamtsystems bestehend aus dem übergeordneten Berechtigungsherausgeber 1, den nachgeordneten Berechtigungsherausgebern 2i, den Registrierungsstellen 4i, den Registriereinrichtungen 6i, und berechtigten Bedienungspersonen Bi ist eine sichere ID - ID1, ID2, ID4, ID6 und IDBi - zugeordnet. Zusätzlich können auch noch den einzelnen Hardwarekomponenten Ki der Registriereinrichtung 6 sichere ID - IDKi - zugeordnet werden. Die sichere ID kann beispielsweise ein elektronischer Schlüssel, ein Zertifikat, ein PC-Dongel, etc. sein.

[0043] In dem übergeordneten Berechtigungsherausgeber 1 wird eine Liste aller ID2 der mit diesem Berechtigungsherausgeber verbundenen nachgeordneten Berechtigungsherausgebern 2 geführt und verwaltet. Bei Kommunikation zwischen dem übergeordneten Berechtigungsherausgeber 1 und einem der nachgeordneten Berechtigungsherausgeber 2i identifizieren sich die beiden Komponenten anhand ihrer jeweiligen ID - ID1 und ID2i. Ebenso wird bei den jeweiligen nachgeordneten Berechtigungsherausgebern 2i eine Liste der sicheren ID4i der jeweils zugeordneten Registrierungsstellen 4i geführt. Bei Kommunikation zwischen dem jeweiligen Berechtigungsherausgeber 2i und einer zugeordneten Registrierungsstelle 4i identifizieren sich die beiden Komponenten wieder anhand der sicheren ID2i bzw. ID4i. Ebenso wird in den Registrierungsstellen 4i eine Liste mit den sicheren IDBi der an die jeweilige Registrierungsstelle 4i angeschlossenen Registriervorrichtungen 6i verwaltet. Zusätzlich können auch noch die einzelnen Komponenten Ki der Registriereinrichtung 6i mit sicheren IDKi versehen werden. Damit wird gewährleistet, daß nur "bekannte" und "geeignete" Komponenten Ki an die Registriereinrichtungen 6i angekoppelt bzw. in diese eingekoppelt werden.

[0044] Zusätzlich muß sich das Bedienpersonal Bi, die die Registriereinrichtungen 6i bzw. deren Komponenten Ki bedient ebenfalls durch eine Sichere ID - IDBi - ausweisen. Beziehungsweise es kann sich nur mit einer derartigen sicheren ID in die jeweilige Komponente Ki bzw. in die Registriereinrichtung 6i einloggen. Die Bedienerberechtigung IDBi kann entweder von dem Berechtigungsherausgebern 1, 2 oder von den jeweiligen Registriereinrichtung 6i oder den jeweiligen Registrierungsstellen 4i vergeben werden.

[0045] Die jeweiligen sicheren ID können bei jeder Kommunikation zwischen den einzelnen Komponenten abgefragt und ausgetauscht werden. Alternativ erfolgt Abfrage und Austausch der sicheren ID nach einem bestimmten Zeitschema oder bei vorliegen von bestimmten Ereignissen. Die Abfrage der Berechtigungs-ID IDBi der Bedienungspersonen Bi erfolgt beim Start der Anwendung "Identifizierung/Registrierung", beim Einloggen der jeweiligen Person oder wiederholt nach einem bestimmten zeitlichen Schema oder bei jedem neuen Registrierungsvorgang.

[0046] Die Registrierung einer zu registrierenden Person bzw. der Betrieb einer Registriereinrichtung 6 kann sowohl in einem Bedienermodus als auch bei unkritischen Anwendungen in einem Selbstbedienungsmodus erfolgen. Im Selbstbedienungsmodus wird die zu registrierende Person über Bildschirm, Tastatur und Lautsprecher durch die einzelnen Registrierungsschritte geführt. Im Bedienermodus ist eine Bedienerperson anwesend, die die einzelnen Registrierungsschritte durchführt und bestimmte Überprüfungen vornimmt.

[0047] Das erfindungsgemäße System bietet in seiner bevorzugten Ausgestaltung folgende Voraussetzungen für die sichere Identifizierung und Registrierung von Personen :

1. Das 4-Augenprinzip wird durch ein nicht manipulierbares Gerät mit den Kernkomponenten Identifizierung, Autentifizierung und Verifizierung und den Hilfskomponenten scannen und lesen von Dokumenten sowie Erfassen von aktuellen biometrischen Merkmalen (Foto, Unterschrift, Fingerprint, Iris, etc.).
2. Das sichere Gerät ist eine entsprechend sichere Umgebung (Fig 3). Dabei sollte das Gerät zur Funktionstüchtigkeit den autentifizierten Kontakt mit einem von einer Route zertifizierten Berechtigungsherausgeber, wie einem zertifizierten Trustcenter, verlangen. Der Verkauf eines solchen Gerätes an Personen mit Fälschungsabsicht bei der Ausgabe digitaler Signaturkarten oder anderer Berechtigungen ist dadurch unschädlich.
3. Das Gerät ermöglicht ein vorzugsweise zertifiziertes Verfahren zum Ausgeben von Berechtigungsmitteln.
4. Es gibt nur einen Verantwortlichen d.h. der Vorgang wird in Beisein nur einer verantwortlichen Person durchgeführt.

Bezugszeichenliste:

[0048]

1	übergeordneter Berechtigungsherausgeber
2i	nachgeordneter Berechtigungsherausgeber
4i	Registrierungsstelle
6i	Registriereinrichtung
8	Steuereinheit
9	Bildschirm
10	Eingabemittel, wie Tastatur etc.
12	Drucker
14	erster Dokumentenleser
15	zweiter Dokumnetenleser
16	Einrichtung zur aktuellen Erfassung eines biometrischen Merkmals
18	Verifikationseinheit
20	Kartenbezahlungseinheit
22	PIN-Eingabeeinheit
23	Einrichtung zur Digitalisierung einer Unterschrift
24	Chipkarten-Beurbeitungseinrichtung
26	PIN-Ausgabedrucker
27	Kartenpersonalisiereinheit
28	DFÜ-Schnittstelle
30	Authentifizierungseinheit
32	unterbrechungsfreie Stromversorgung
34	externe Datenbanken
36	interne Datenbanken
Bi	berchtigte Bedienungspersonen
Ki	Komponenten von Bi
ID1	sichere ID von 1
ID2i	sichere ID von 2i
ID4i	sichere ID von 4i
ID6i	sichere ID von 6i
IDKi	sichere ID von Ki

Patentansprüche

1. System zur sicheren Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungsmitteln wie einer digitalen Signaturkarte, mit:

   - wenigstens einem Berechtigungsherausgeber (1, 2) mit einer EDV-Anlage,
   - wenigstens einer Registrierungsstelle (4) mit einer Registriereinrichtung (6),
   - wobei die EDV-Anlagen des Berechtigungsherausgebers (1, 2) und die Registriereinrichtung (6) der Registrierungsstellen (4) mittels DFÜ miteinander verbunden und in ein Authentifikationssystem (30, ID) eingebunden sind,
   - wobei die Registriereinrichtung (6) der wenigstens einen Registrierungsstelle (4) wenigstens eine Identifikationseinheit (14, 15, 16, 23), wenigstens ein Ausgabemittel (9, 12), wenigstens ein Eingabemittel (9, 10) und eine Steuereinheit (8) umfaßt,
   - wobei die Identifikationseinheit (14, 15, 16, 23) einen Dokumentenleser (14, 15) zum Lesen von die zu registrierende Person identifizierenden Dokumenten, wie z. B. einem amtlichen Ausweis, und ein Mittel (16) zur aktuellen Erfassung biometrischer Daten der zu registrierenden Person aufweist.

2. System nach Anspruch 1, gekennzeichnet durch wenigstens eine Verifikationseinheit (18), die (18) auf den durch den Dokumentenleser (14, 15) erfaßten identifizierenden Dokumenten enthaltene biometrischen Merkmalen mit den durch die Identifikationseinheit (14, 15, 16) erfaßten biometrischen Merkmalen auf Übereinstimmung vergleicht und anhand einer voreingestellten Identitätswahrscheinlichkeit das Ergebnis der Verifikation feststellt.

3. System nach Anspruch 1 oder 2, gekennzeichnet durch eine Verifikationseinheit (18), welche die inhaltliche Echtheit der identifizierenden und/oder beschreibenden Dokumente überprüft, indem die das entsprechende Dokument ausstehende Institution per DFÜ angefragt wird, ob das jeweilige Dokument mit genau diesen Merkmalen tatsächlich ausgegeben worden und noch gültig ist.

4. System nach Anspruch 1,2 oder 3 gekennzeichnet durch wenigstens einen übergeordneten Berechtigungsherausgeber (1) mit einer EDV-Anlage.

5. System nach Anspruch 1,2,3 oder 4, dadurch gekennzeichnet, daß auf den EDV-Anlagen der Berechtigungsherausgeber (1, 2) und/oder der Registriereinrichtungen (6) der Registrierungsstellen (4) Programme und Daten für die sichere Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungen, wie einer digitalen Signaturkarte, von anderen Anwendungen virtuell oder physisch getrennt sind.

6. System nach Anspruch 1,2,3,4 oder 5, dadurch gekennzeichnet, daß die Registriereinrichtungen (6) der Registrierungsstellen (4) ausschließlich für die sichere Identifikation und Registrierung von Personen, insbesondere für die Herausgabe von personenbezogenen Berechtigungen wie einer digitalen Signaturkarte genutzt werden.

7. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Identifikationseinheit (14, 15, 16, 23) der Registrierungsstellen (4) eine Einrichtung zur Echtheitsprüfung der durch den Dokumentenleser (14) erfaßten Dokumente aufweist.

8. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß Berechtigungsherausgeber (1, 2) und/oder Registrierungsstellen (4) mittels einer sicheren ID (ID1, ID2I, ID4I) in Form eines elektronischen Schlüssels eindeutig identifizierbar sind.

9. System nach Anspruch8, dadurch gekennzeichnet, daß EDV-Anlagen bzw. Komponenten davon der Berechtigungsherausgeber (1, 2) und/oder die Registriereinrichtungen (6) der Registrierungsstellen (4) mittels einer sicheren ID (ID6I, ID4I) in Form eines elektronischen Schlüssels eindeutig identifizierbar sind.

10. System nach Anspruch 8 oder 9, dadurch gekennzeichnet, daß die sichere ID ein elektronisches Zertifikat und/oder eine digitale Signatur und/oder eine Hardware-Komponente ist.

11. System nach einem der vorhergehenden Ansprüche 8 bis 10, dadurch gekennzeichnet, daß die Ausgabe der sicheren ID (ID1, ID2I) der Berechtigungsherausgeber (1, 2) durch den übergeordneten Berechtigungsherausgeber (1) erfolgt.

12. System nach einem der vorhergehenden Ansprüche 8 bis 11, dadurch gekennzeichnet, daß die Ausgabe der sicheren ID (ID6I) der Registrierungsstellen (6) durch den Berechtigungsherausgeber (2) erfolgt.

13. System nach einem der vorhergehenden Ansprüche 8 bis 12, dadurch gekennzeichnet, daß die sichere ID durch die ausgebende Stelle periodisch oder bei bestimmten Ereignissen überprüft wird.

14. System nach einem der vorhergehenden Ansprüche 8 bis 13, dadurch gekennzeichnet, daß die Registriereinrichtung (6I) der Registrierungsstellen (4) nur bei Vorliegen einer sicheren ID der jeweiligen Registrierungsstelle (4) und einer sicheren ID des zugehörigen Berechtigungsherausgebers (1, 2) funktionsfähig ist

15. System nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Bedienung der EDV-Anlagen und/oder der Registriereinrichtungen (6) nur durch berechtigte Personen (5I) mit einer entsprechenden sicheren ID (ID5I) möglich ist.

16. Registriereinrichtung, insbesondere für ein System nach einem der Ansprüche 1 bis 15, mit wenigstens einer Identifikationseinheit (14, 15, 16, 23), wenigstens einer Verifikationseinheit (16), wenigstens einem Ausgabemittel (9, 12), wenigstens einem Eingabemittel (9, 19) und einer Steuereinheit (6).

- wobei die Identifikationseinheit (14, 15, 16, 23) einen Dokumentenleser (14, 15) zum Lesen von die zu registrierende Person identifizierenden Dokumenten, wie z. B. einem amtlichen Ausweis, und ein Mittel (16) zur aktuellen Erfassung biometrischer Daten der zu registrierenden Person aufweist, und
- wobei die Verifikationseinheit (16) auf den durch den Dokumentenleser (14, 15) erfaßten identifizierenden Dokumenten enthaltene biometrischen Merkmalen mit den durch die Identifikationseinheit (14, 15, 16, 23) erfaßten biometrischen Merkmalen auf Übereinstimmung vergleicht und anhand einer voreingestellten Identitätswahrscheinlichkeit das Ergebnis der Verifikation feststellt.

17. Registriereinrichtung nach Anspruch 16, gekennzeichnet durch einen weiteren Dokumentenleser (15).

18. Registriereinrichtung nach Anspruch 16 oder 17, gekennzeichnet durch eine Einrichtung (20) zum Bezahlen, insbesondere durch ein EFTPOS-Terminal und/oder einer Schnittstelleneinrichtung (28) für den Zugriff auf interne und/oder externe Datenbanken und Register(34, 36).

19. Registriereinrichtung nach einem der Ansprüche 16 bis 18, gekennzeichnet durch eine Bearbeitungseinrichtung (24, 27) für Berechtigungsmittel, insbesondere in Form von Chipkarten.

20. Registriereinrichtung nach einem der Ansprüche 16 bis 19, dadurch gekennzeichnet, daß die Identifikationseinheit (14, 15, 16, 23) eine Einrichtung (23) zum Erfassen der Dynamik eines biometrischen Merkmals umfaßt.

21. Verfahren zum Betreiben eines Systems zur sicheren Identifikation und Registrierung von Personen für die Ausgabe von personenbezogenen Berechtigungsmitteln nach einem der vorhergehenden Ansprüche mit den Verfahrensschritten:

a) Einlegen eines die zu registrierende Person identifizierenden Dokuments in den Dokumentenleser (14, 15), wobei das identifizierende Dokument wenigstens ein biometrisches Merkmal der zu registrierenden Person enthält;
b) Einlesen der Personendaten von dem identifizierenden Dokument;
c) Übernehmen des wenigstens einen biometrischen Merkmals der zu registrierenden Person von dem identifizierenden Dokument;
d) aktuelle Erfassung wenigstens eines biometrischen Merkmals der zu registrierenden Person, wobei wenigstens eines der aktuell

erfaßten biometrischen Merkmale in Schritt c) von dem identifizierenden Dokument übernommen worden ist;

e) Überprüfen der Daten von dem identifizierenden Dokument mit den aktuell erfaßten Daten auf Übereinstimmung;

f) Feststellen der Identität bei Übereinstimmung in Schritt e) mit einer bestimmten Wahrscheinlichkeit; und

g) Freigabe des gewünschten personenbezogenen Berechtigungsmittels zur Ausgabe.

22. Verfahren nach Anspruch 21, gekennzeichnet durch den weiteren Verfahrensschritt:

Überprüfen der physischen Echtheit des identifizierenden Dokuments.

23. Verfahren nach einem der Ansprüche 21 oder 22, gekennzeichnet durch den weiteren Verfahrensschritt: Einlesen von wenigstens einem weiteren die zu identifizierende Person beschreibenden Dokument der zu registrierenden Person.

24. Verfahren nach einem der Ansprüche 21 bis 23, dadurch gekennzeichnet, daß von dem weiteren Dokument Attribute der zu registrierenden Person wie Vollmachten, Berechtigungen etc., eingelesen werden.

25. Verfahren nach einem der Ansprüche 21 bis 24, gekennzeichnet durch den weiteren Verfahrensschritt:

Überprüfen der inhaltlichen Echtheit des identifizierenden Dokuments indem die das identifizierende Dokument ausstellende Institution per DFÜ angefragt wird, ob das jeweilige identifizierende Dokument mit genau diesen Merkmalen tatsächlich ausgegeben worden ist und noch gültig ist.

26. Verfahren nach einem der Ansprüche 21 bis 25, gekennzeichnet durch den weiteren Verfahrensschritt:

Auswahl der gewünschten Registrierung bzw. des gewünschten Berechtigungsmittels zu Beginn der Registrierung.

27. Verfahren nach einem der Ansprüche 21 bis 26, gekennzeichnet durch den weiteren Verfahrensschritt:

Ergänzen der personenbezogenen Daten aus vorhandenen Datenbeständen und/oder durch dialoggeführte Rückfrage bei der zu registrierenden Person.

28. Verfahren nach einem der Ansprüche 21 bis 27, dadurch gekennzeichnet, daß die erfaßten Daten, Merkmale und sonstige Angaben auf einen Anzeigeeinrichtung angezeigt werden.

29. Verfahren nach einem der Ansprüche 21 bis 28, dadurch gekennzeichnet, daß die erfaßten Daten, Merkmale und sonstige Angaben ausgedruckt werden.

30. Verfahren nach einem der Ansprüche 21 bis 29, dadurch gekennzeichnet, daß die erfaßten Daten, Merkmale und sonstige Angaben in Form eines Antrags angezeigt und/oder ausgedruckt werden.

31. Verfahren nach einem der Ansprüche 21 bis 30, dadurch gekennzeichnet, daß der Registrierungsvorgang durch die zu registrierende Person mittels Unterschrift bestätigt wird, daß die geleistete Unterschrift mit der auf dem identifizierenden Dokument befindlichen Unterschrift verglichen wird, und daß bei ausreichender Übereinstimmung die Freigabe der gewünschten Registrierung erfolgt.

32. Verfahren nach einem der Ansprüche 21 bis 31 zur Ausgabe einer digitalen Signaturkarte, gekennzeichnet durch die zusätzlichen Verfahrensschritte:

A) Auslesen der von dem Berechtigungsherausgeber für die Zertifikatserstellung und Bearbeitung benötigten PSE-Daten aus einer vorinitialisierten Chipkarte in einem entsprechend hoch zertifizierten Kartenlese/Kartenschreibgerät;

B) Export der erfaßten Daten der zu registrierenden Person in ein den gesetzlichen Regelungen entsprechendes Software-Programm;

C) Zuordnen der Daten der zu registrierenden Person zu den PSE-Daten;

D) Zusammenstellen der von dem Berechtigungsherausgeber benötigten Daten und Anzeige auf einer gesetzeskonformen Anzeigeeinrichtung;

E) Signieren, Verschlüsseln und Übertragen dieser Daten an den Berechtigungsherausgeber;

F) Bearbeiten durch den Berechtigungsherausgeber und Übermitteln der zur Erstellung der Signaturkarte benötigten Daten, wie Zertifikat oder Freigabecodes, digital signiert und verschlüsselt an die Registrierungsstelle;

G) Entschlüsselung und Überprüfung der von dem Berechtigungsherausgeber übermittelten Daten;

H) Falls die Überprüfung in Schritt G) positiv ist: Personalisieren und Übertragen der erforderlichen Daten mit Zertifikat auf die vorinitialisierte Chipkarte;

I) Belehrung der zu registrierenden Person entsprechend den gesetzlichen Regelungen; und

J) Ausdruck von vorzugsweise zwei Bestätigungen über die erfolgte Belehrung und Bestätigung des Erhalts der digitalen Signaturkarte.

33. Verfahren nach Anspruch 32, gekennzeichnet durch die weiteren Verfahrensschritte:

Überprüfung der Einmaligkeit des in den PSE-Daten der vorinitialisierten Chipkarte enthaltenen Schlüssels durch den Berechtigungsherausgeber.

34. Verfahren nach Anspruch 32 oder 33, dadurch gekennzeichnet, daß in Schritt E) auch das Prüfungsergebnis an den Berechtigungsherausgeber übertragen wird

35. Verfahren nach einem der Ansprüche 32 bis 34, dadurch gekennzeichnet, daß die digitale Signaturkarte erst ausgegeben wird, wenn die zu registrierende Person die PIN der digitalen Signaturkarte ändert.

36. Verfahren nach einem der Ansprüche 32 bis 35, dadurch gekennzeichnet, daß die Belehrung in Schritt I) in Form einer programmierten, dialoggeführten Unterweisung mit Test erfolgt und daß die digitale Signaturkarte nur aktiviert wird, wenn die zu registrierende Person die programmierte Unterweisung mit Test erfolgreich abschließt hat.

37. Verfahren nach einem der Ansprüche 21 bis 36, dadurch gekennzeichnet, daß eine Bestätigungsmeldung an eine dritte Person erzeugt wird, die Berechtigungen, insbesondere Vertretungsmacht, für die jeweilige zu registrierende Person und das jeweilige Berechtigungsmittel erteilt hat, wobei die Angaben über die Berechtigungen auf dem Berechtigungsmittel gespeichert werden.

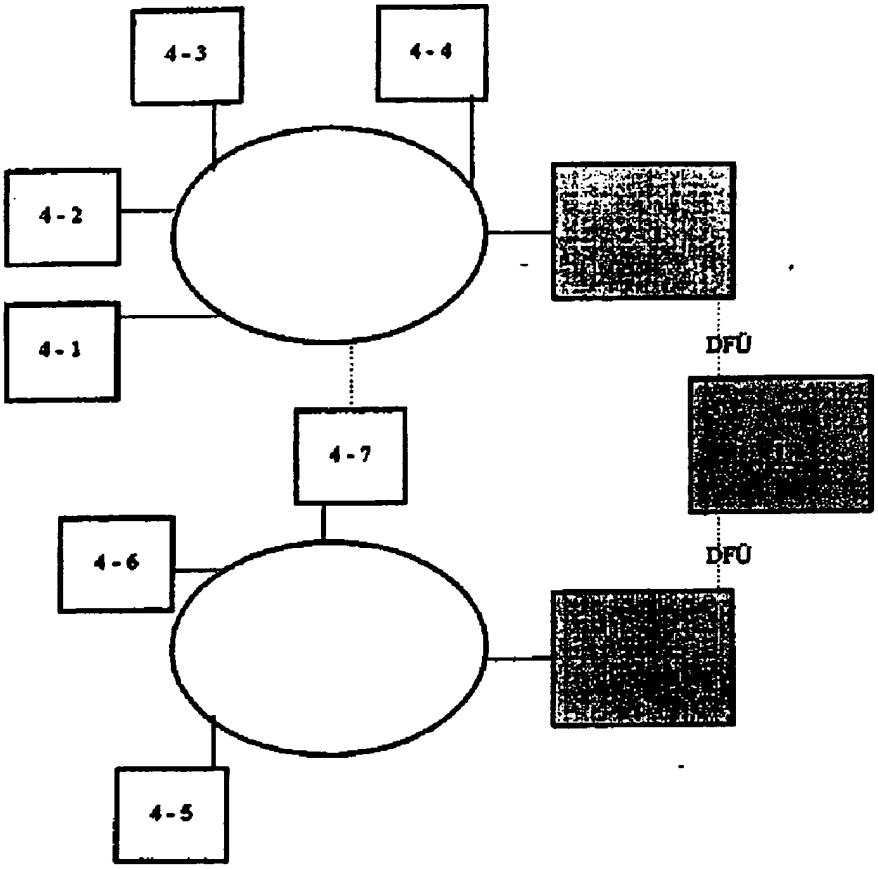
38. Verfahren nach einem der Ansprüche 21 bis 37, dadurch gekennzeichnet, daß die Registrierung nach Abschluß der Registrierung oder nach Ablauf einer bestimmten Zeitdauer beendet wird.

39. Verfahren nach einem der Ansprüche 21 bis 38, dadurch gekennzeichnet, daß die Registrierungsstellen alle Registrierungsvorgänge protokollieren, daß die Protokolle mit den dazugehörigen personenbezogenen Daten und geforderten Dokumenten nach einem bestimmten Schema an den Berechtigungsherausgeber übermittelt werden, und daß der Berechtigungsherausgeber die Protokolle, Dokumente und die Daten hinsichtlich Lesbarkeit und Vollständigkeit überprüft.

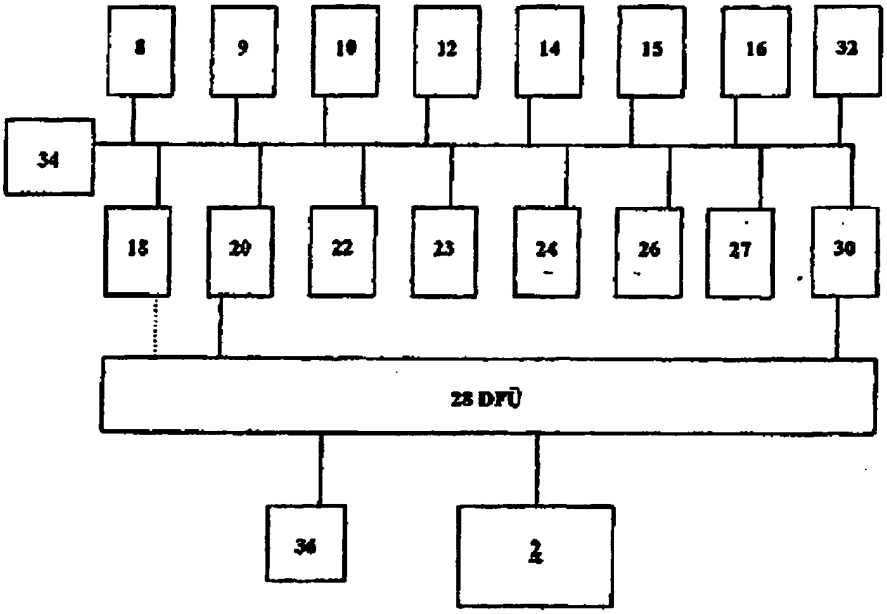
40. Verfahren nach einem der Ansprüche 21 bis 39, dadurch gekennzeichnet, daß die in den Registrierungsstellen ermittelten und erfaßten Daten und Dokumente nach einem bestimmten zeitlichen Schema gelöscht werden.

41. Verfahren nach einem der Ansprüche 21 bis 40, dadurch gekennzeichnet, daß die in den Registrierungsstellen ermittelten und erfaßten Daten und Dokumente nach Löschungsfreigabe durch den Berechtigungsherausgeber gelöscht werden.

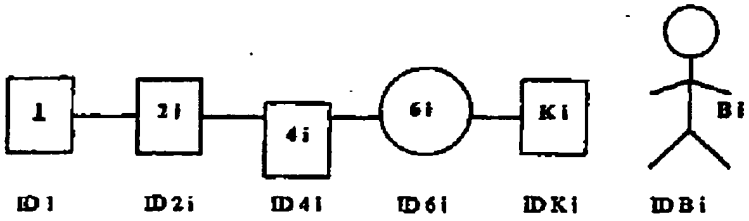
Figur 1



Figur 2



Figur 3



European Patent Application No. 0 999 528 A2

Job No.: 7168-106589 Ref.: EP0999528A
Translated from German by the McElroy Translation Company
800-531-9977 customerservice@mcelroytranslation.com